REMARKS

The Notification of Non-Compliant Amendment dated November 14, 2008, states that the amendments to the specification and claims do not accurately reflect the changes made relative to the prior version. The specification paragraph and the claims listed above now accurately reflect the changes made relative to the prior version.

Claims 1-17 have been examined, with all claims rejected.

The disclosure has been objected to because of informalities. The amendments to the specification as believed to overcome this objection.

Claims 1-17 have been rejected under 35 USC 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,768,382; hereinafter "Schneier") in view of Obana et al. (JP 11338993; hereinafter "Obana").

Applicant has amended the claims to conform with the claims of the parallel Japanese patent application, based on which this Japanese application has been granted in view of Obana.

Obana seeks to improve a terminal/IC-card system in which encrypted encryption/decryption programs for communicating with IC-cards are stored in the terminal. For communicating with an IC-card, the terminal transmits the respective encrypted version of the encryption/decryption program to the IC-card whereupon the IC-card decrypts the program and sends back the decrypted version of the program to the terminal. In executing the decrypted version of the encryption/decryption program for communicating with the IC-card during the session, the terminal stores the decrypted version in a volatile memory only.

Obana seeks to improve the system in two ways. Firstly, Obana proposes a system avoiding the necessity to store a large amount of different encrypted encryption/decryption programs in the terminals. Secondly, Obana seeks to avoid the transmission of the decrypted version of the encryption/decryption program from the IC-card back to the terminal (see paragraphs [0004] to

[0008]). Accordingly, in the system of Obana, the IC-cards are dedicated for registering different encryption/decryption programs in either a RAM 250 or an EEPROM 240. Each of these programs is indexable by the terminal by means of an encryption/decryption program identifier. Moreover, in the system of Obana, the terminals are not only capable of registering new encryption/decryption programs onto the IC-cards but to delete existing encryption/decryption programs from the IC-cards. In this regard, Obana describes that an active deletion of an encryption/decryption program stored in the volatile memory RAM 250 is not necessary (see paragraph [0037]).

Neither Obana nor Schneier describes or suggests splitting up a cryptographic algorithm code into two parts, one of which being stored in the non-volatile memory of a security module, the other one of which is to be transferred from the terminal to the security module and stored in the volatile memory of the security module, as required by the claimed invention. Moreover, none of the applied references suggests a splitting-up of cryptographic algorithm codes into two parts, one part of which is stored in a non-volatile memory while the other part is stored in the volatile memory, the latter one consisting of memory addresses of computing components necessary for performing the algorithm code or jump addresses of the algorithm code pointing to partial routines within the remainder of the algorithm code, as also required by the claimed invention. In particular, none of the prior art documents addresses problems occurring with the repeated transfer of an algorithm code from a terminal to the IC-card while concurrently substantially maintaining the level of security.

With respect to claims 5 and 8, the subject matter of which has been amended into the independent claims, the Examiner states: "Schneier and Obana further disclose a memory managing unit and code that include addresses (Schneier, column 7, lines 48-61; Obana, paragraph [0031])." However, column 7, lines 48-61, of Schneier reads as follows:

> Referring now to Fig. 4A there is shown a schematic of a portion of an illustrative memory arrangement and some hardware for the game computer 14 in the system of the present invention. For convenience, the internal memory 23 of a personal computer 14 is shown. The memory 23 includes RAM and ROM and is coupled to a central processing unit ("CPU") 27 in a conventional manner, and includes a typical operating system (not shown). The CPU 27 and related hardware are

> typically referred to as a processor. We use the term "associated memory" to indicate that the game computer memory includes both internal and external memory devices such as CD-ROM drives and the like. The processor executes programs from memory in a conventional manner.

Nothing in this portion of Schneier teaches or suggests the features in question. Contrary to the assessment of the Examiner, neither Fig. 4A nor the portion of the description mentioned by the Examiner indicates the existence of a memory managing unit or a code that explicitly includes addresses. Schneier merely states: "The processor executes programs from memory in a conventional manner." Further, Schneier does not disclose any sub-division of a program or algorithm code into two parts, namely a "first part of the algorithm code consisting of memory addresses, or computing components necessary for performing the algorithm code, and/or jump addresses of the algorithm code, pointing to partial routings within the remainder of the algorithm code." In other words, Schneier does not disclose any separation of memory addresses or jump addresses from an algorithm code in order to treat this separated portion of the algorithm code separately from the remainder. The idea underlying the amended independent claims is, however, that the remainder of the algorithm code stored in the non-volatile memory of the security module and thereby being liable to an investigation by unauthorized third parties, is of no value to the unauthorized third party if they do not have access to the memory addresses and/or jump addresses used by this algorithm code. Restricting the part of the algorithm code to be transferred from the terminal to the security module to memory addresses and/or jump addresses, however, alleviates the overhead in the communication between the terminal and the security module and therefore, reduces the terminal session times.

This deficiency in disclosing the afore-mentioned differential features is also true for Obana. The English translation of paragraph [0031] of Obana annexed to the Office Action is not readable. Therefore, a translation of paragraphs 17-32 of Obana are attached herewith in order to complement the translation of paragraphs [0033] to [0045] that has already been provided along with the IDS. It is clear from this English translation that this paragraph does not suggest any sub-division of a program code in a manner as set out in the last paragraph of the independent claims as attached herewith.

The claims are patentable over the applied references for at least these reasons. Reconsideration and withdrawal of the prior art rejection is therefore respectfully requested.

In view of the above, Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: July 9, 2009

Respectfully submitted,
/Laura C. Brutman/
By_____
Laura C. Brutman
Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant